Ivanti: automatyzacja pracy działu IT

Dzięki oprogramowaniu Ivanti Endpoint Manager możliwe jest znaczne ograniczenie wykonywania powtarzalnych zadań przez pracowników działu IT oraz zapewnienie wysokiego poziomu bezpieczeństwa firmowych danych.

Dla administratorów IT zarządzanie infrastrukturą teleinformatyczną jest jednym z najbardziej rutynowych działań, ale też związanym z bardzo dużą odpowiedzialnością. Elementów tej pracy jest wiele: inwentaryzacja sprzętu i oprogramowania, obsługa systemów do administrowania zasobami, licencjami, dbałość o instalację aktualizacji i in. Aby wymienione zadania były wykonane poprawnie, konieczne jest posiadanie wiedzy o zgromadzonych w przedsiębiorstwie zasobach IT, stosowanych regułach polityki bezpieczeństwa oraz uprawnieniach przyznanych użytkownikom.

Niemałym problemem w firmach jest brak czasu na rzetelne wykonywanie zadań związanych z zarządzaniem IT – wystarczy sobie wyobrazić konieczność zaktualizowania systemu operacyjnego lub aplikacji na tysiącu komputerów i późniejszą weryfikację poprawności przebiegu tego procesu. Dziś w większości przedsiębiorstw odbywa się to ręcznie, więc administratorzy nie zajmują się ważniejszymi rzeczami niż bieżąca obsługa infrastruktury.

Tymczasem zarządzanie środowiskiem IT można w dość prosty sposób zautomatyzować za pomocą narzędzi dostępnych w portfolio firmy Ivanti. Możliwe jest stworzenie katalogu świadczonych w sposób automatyczny usług, z których korzystają użytkownicy, np. wnioskowanie o udostępnienie licencji dla jakiejś aplikacji i jej automatyczna instalacja, przypisanie uprawnień użytkownika itd. Dzięki temu zespoły IT oszczędzają wiele czasu, ale nie tracą kontroli nad całym środowiskiem.

Wszechstronne zarządzanie końcówkami

Rozwiązanie Ivanti Endpoint Manager (wcześniej dostępne jako Landesk Management Suite) zapewnia zinwentaryzowanie sprzętu, wirtualnych maszyn i oprogramowania tworzących środowisko IT klienta oraz prowadzenie analizy jego użytkowania. Moduł Software License Monitoring umożliwia kontrolowanie liczby uruchomień danej aplikacji przez każdego użytkownika oraz czasu jej użytkowania. Pomaga to w monitorowaniu stopnia wykorzystania posiadanych licencji – jeżeli pracownik nie sięgnie po daną aplikację przez określony czas, można ją automatycznie odinstalować i w ten sposób „odzyskać" licencję dla innego, np. nowozatrudnionego użytkownika. Może też się zdarzyć, że liczba posiadanych licencji przekracza potrzeby firmy i z części można zrezygnować, zmniejszając tym samym wartość opłat za wsparcie lub aktualizacje, wnoszonych na rzecz producenta danego oprogramowania. Software License Monitoring odpowie też na pytanie czy na urządzeniach zainstalowana jest odpowiednia ilość oprogramowania w stosunku do zakupionych licencji.

Jeżeli u klienta zainstalowane jest środowisko Active Directory, w którym odzwierciedlono strukturę firmy, to Ivanti Endpoint Manager może wspierać proces przygotowania stanowisk dla nowych pracowników. Po dopisaniu tych ostatnich do odpowiedniej grupy w AD, automatycznie na ich komputerze umieszczany jest odpowiedni obraz systemu operacyjnego z aplikacjami. Natomiast jeśli pracownik zmieni stanowisko, a więc także grupę w Active Directory, na jego sprzęcie też zostaną dokonane odpowiednie zmiany.

9 kroków zapewniających bezpieczeństwo w środowisku IT

Specjaliści FBI przygotowali dziewięć porad dla firm, które chcą zwiększyć poziom ochrony swojego środowiska IT przed zagrożeniami, w tym ransomware'em.

- Aktualizuj systemy operacyjne i aplikacje.
- Upewnij się, że masz aktualnego antywirusa.
- Kontroluj uprzywilejowane konta.
- Stosuj kontrolę dostępu bazującą na rodzaju danych.
- Kontroluj uprawnienia aplikacji.
- Wyłącz możliwość tworzenia makr w aplikacjach Microsoft Office.
- Twórz białe listy aplikacji.
- Korzystaj ze środowisk wirtualnych lub kontenerów.
- Regularnie rób backup.

ivanti

Jednym z podstawowych sposobów ochrony środowisk IT przed zagrożeniami jest obecnie aktualizowanie systemów operacyjnych i aplikacji. Proces ten został umieszczony na pierwszym miejscu 9-punktowej listy przygotowanej przez FBI wraz z kilkoma dużymi firmami IT, rekomendującej działania minimalizujące ryzyko zarażenia infrastruktury IT złośliwym kodem oraz wycieku danych (szczegóły w ramce na stronie obok). Ivanti proponuje swoim klientom przeznaczony dla Endpoint Managera moduł Ivanti Patch Management, który w bardzo dużym stopniu automatyzuje i wspiera proces wgrywania poprawek i aktualizacji do posiadanego przez firmę oprogramowania, zarówno na urządzeniach końcowych, jak i serwerach z systemami Windows, Linux, Unix, Solaris i macOS.

Obiektem tych wszystkich działań mogą być również komputery, które nie są na stałe podłączone do firmowej sieci, np. laptopy handlowców, od czasu do czasu podłączających się do Internetu i zdalnie korzystających z korporacyjnych zasobów. Wtedy moduł Cloud Services Appliance jest w stanie wymusić na tych komputerach dokonanie stosownych aktualizacji lub wgranie nowych reguł polityki bezpieczeństwa.

Ivanti – do usług

Partnerzy Ivanti mogą korzystać z narzędzi tego producenta do świadczenia swoim klientom usług w zakresie kontroli ich infrastruktury IT lub zdalnego zarządzania nią oraz wdrożonymi procedurami, które poddane zostały automatyzacji. Współpraca z klientami w tym obszarze może odbywać się na dwa sposoby. W pierwszym to klient kupuje licencję na korzystanie z danego narzędzia Ivanti i posiada ją, ale zleca obsługę swojego środowiska firmie trzeciej z wykorzystaniem tego oprogramowania. W drugim to partner producenta kupuje odpowiednią liczbę licencji i korzysta z nich w celu obsługi swoich klientów, których infrastruktura może znajdować się w dowolnym miejscu (u klienta, partnera lub w chmurze). Dla każdego z nich może zastosować inne reguły polityki bezpieczeństwa oraz procedury zarządzania środowiskiem. W przypadku zakończenia współpracy z danym klientem licencje wracają do puli i można wykorzystać je u innego.

W tym drugim modelu zapewnione jest pełne bezpieczeństwo i poufność danych przetwarzanych w środowiskach klientów. Jeżeli do obsługi każdej z firm przypisani są inni administratorzy, to zagwarantowane jest, że nie będą mogli oni nawzajem „podglądać" środowisk innych klientów. Ale istnieje też możliwość stworzenia konta superadministratora, który będzie miał wgląd we wszystkie środowiska infrastruktury IT – stosowane jest to np. w grupach kapitałowych, w których istnieje jedno centrum usług wspólnych.

Autoryzowanymi dystrybutorami oprogramowania Ivanti w Polsce są firmy: Alstor, Headtechnology oraz Prianto.

>>> Trzy pytania do...

Bogdana Lontkowskiego, dyrektora regionalnego Ivanti na Polskę, Czechy, Słowację i kraje bałtyckie

CRN Z jakimi wyzwaniami związanymi z zarządzaniem infrastrukturą obecnie najczęściej spotykają się administratorzy IT w przedsiębiorstwach?

Bogdan Lontkowski Z wdrażaniem nowych wersji systemów operacyjnych. Wciąż bardzo dużo jest komputerów z systemami Windows 7/8/8.1, a Windows 10 staje się coraz popularniejszy i bez problemu działa także na starszych komputerach. Całkowite zakończenie wsparcia dla systemu Windows 7 przewidziane jest na styczeń 2020 r., więc firmy muszą się zawczasu przygotować, aby nie narażać swojej infrastruktury na niebezpieczeństwo związane z brakiem aktualizacji. Dlatego warto zainteresować się narzędziami do automatyzacji procesu instalacji i migracji systemów operacyjnych, aby wyeliminować jego czaso- i pracochłonność.

CRN W jakim stopniu tego typu automatyzacja wiąże się z ryzykiem niepowodzenia procesu aktualizacji? Nikt nie chciałby być w skórze administratora, który rano dowiaduje się, że po przeprowadzonych w nocy aktualizacjach nie działa połowa komputerów...

Bogdan Lontkowski Takie ryzyko naturalnie istnieje, dlatego zalecamy szereg działań, które je minimalizują. Aktualizację systemów operacyjnych i oprogramowania należy podzielić na etapy – najpierw przeprowadzić ją w środowisku testowym, a potem na wybranej grupie użytkowników, w przypadku których ewentualny przestój w pracy nie spowoduje dużego zamieszania. Dopiero później można decydować się na „hurtowe" wdrożenie aktualizacji. O minimalizację tego ryzyka w pewnym stopniu dba też Ivanti – przed udostępnieniem klientom w naszym repozytorium paczek z aktualizacjami oprogramowania testujemy je, aby sprawdzić, czy nie ma znaczących błędów. Ale nie jesteśmy w stanie sprawdzić wszystkiego, np. czy po aktualizacji różne aplikacje nie będą wchodziły ze sobą w konflikt. To zadanie administratorów, którzy – działając w środowisku testowym – powinni wykluczyć ryzyko wystąpienia ewentualnych problemów.

CRN Czy taki proces automatycznego wprowadzania poprawek można zastosować także w środowisku serwerowym?

Bogdan Lontkowski Nie rekomendujemy tego. Tak jak wspomniałem, ryzyko wystąpienia problemów jest minimalizowane, ale nie da się wyeliminować go w całości. Dlatego uważamy, że aktualizacji serwerów powinno dokonywać się ręcznie, w zaplanowanym czasie, zdefiniowanym oknie serwisowym i po przeprowadzeniu testów na kopii tych serwerów, np. w środowisku wirtualnym.

Dodatkowe informacje:

Bogdan Lontkowski, dyrektor regionalny na Polskę, Czechy, Słowację i kraje bałtyckie, bogdan.lontkowski@ivanti.com